Method for generating and distributing unpersonalized and confidential electronic keys

Patent Number: EP0730253
Publication date: 1996-09-04
Inventor(s): METTKEN WERNER DIPL-ING (DE); MOOS RAINER (DE)
Applicant(s):: DEUTSCHE TELEKOM AG (DE)
Requested Patent: ☐ EP0730253, A3
Application Number: EP19960101556 19960203
Priority Number(s): DE19951007043 19950301
IPC Classification: G07F7/10 ; G07C9/00
EC Classification: G07C9/00B2, G07F7/10D2
Equivalents: ☐ DE19507043, FI960959, NO960793

Abstract

The code carrier is provided with a visible reference identification and a generally accepted manufacturer PIN and is pre-manufactured with a code. The code contains a component to be kept secret, a specially protected area. It also contains a generator seal and reference information in less protected areas. The fixed, public code components are stored together with a second different reference information at the time of output. When a code is first allocated to a user, this changes the manufacturer PIN into an individual PIN, leaves the code receipt, and verifies its identity of the instant of personalisation, which manages the two references, personalises the public code components, seals them, enters them into the code index, and confirms this with the user.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 730 253 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
04.09.1996 Patentblatt 1996/36

(51) Int. Cl.[6]: **G07F 7/10**, G07C 9/00

(21) Anmeldenummer: **96101556.7**

(22) Anmeldetag: **03.02.1996**

(84) Benannte Vertragsstaaten:
BE CH FR GB LI LU NL SE

(30) Priorität: **01.03.1995 DE 19507043**

(71) Anmelder: **Deutsche Telekom AG**
D-53113 Bonn (DE)

(72) Erfinder:
- **Moos, Rainer**
  D-57080 Siegen (DE)
- **Mettken, Werner, Dipl.-Ing.**
  D-59969 Hallenberg (DE)

(54) Verfahren zur Erzeugung und Verteilung unpersonalisierter vertraulicher elektronischer Schlüssel

(57) **2.1.** Schlüsselträger werden von einer geeigneten Instanz in gesicherter Umgebung erzeugt und personalisiert und enthalten bereits Geheimnis und Erzeugersiegel. Sie sollen in unbegrenzter Zahl im Vorlauf erzeugt und verteilt werden können, ohne die Zertifikate bei der Personalisierung mit dem Geheimnis zusammen in einen Schlüsselträger zu schreiben und ohne daß die Identität des späteren Inhabers oder die Anwendung bekannt bzw. festgelegt sind.

2.2. Die Schlüsselträger werden mit einer sichtbaren Referenzidentifikation, einer Hersteller-PIN und einem Schlüssel vorproduziert der eine geheimzuhaltende Komponente im besonders geschützten Bereich sowie ein Erzeugersiegel und eine Referenzinformation im weniger geschützten Bereich enthält. Die fest zugehörige öffentliche Schlüsselkomponente wird zusammen mit einer zweiten ungleichen Referenzinformation bei der Ausgabeinstanz gespeichert. Erst bei der Zuordnung des Schlüssels zu einem Benutzer ändert er die Hersteller-PIN in eine Individual-PIN und weist seine Identität gegenüber der Personalisierungsinstanz aus, welche beide Referenzen verwaltet, die öffentliche Schlüsselkomponente personalisiert, versiegelt, in das Schlüsselverzeichnis einträgt und dem Benutzer bestätigt.

2.3. Die nach diesem Verfahren hergestellten Schlüssel sind universell anwendbar.

EP 0 730 253 A2

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren nach dem Oberbergriff des Patentanspruchs 1. Derartige Verfahren sind aus vielen Anwendungsbereichen elektronischer Schlüssel bekannt.

Bisherige Konzepte zur vertrauenswürdigen Absicherung von Informationen mit kryptographischen Verfahren gehen davon aus, daß eine geeignete Instanz in gesicherter Umgebung Schlüssel erzeugt, personalisiert, d. h. mit einer Identität verknüpft, und in ein gesichertes Medium verbringt. Die personalisierende Instanz verwaltet, pflegt und verteilt die Verknüpfungsinformation (Zertifikat). Der Benutzer des Verfahrens wendet das Schlüsselsystem an und verteilt damit verbunden seine eigene Identität.

Zur Zeit der Schlüsselerzeugung müssen alle notwendigen Daten zur Personalisierung des Schlüssels bekannt sein. Dies bedeutet, daß nicht mit Vorlauf gearbeitet werden kann. Weiterhin sind so erzeugte Schlüsselträger (z.B. Chipkarten) sofort sicherheitskritische Komponenten, da sie das Geheimnis und das Zertifikat enthalten. Ebenso ist zu diesem Zeitpunkt auch die ggf. notwendige persönliche Identifikationsnummer (PIN) dem Personalisierer bekannt.

Um dem Inhaber des Schlüssels Vertrauenswürdigkeit zu gewährleisten, muß ein sehr großer organisatorischer und technischer Aufwand zur Geheimhaltung dieser Informationen betrieben werden.

Eine Verbesserung gegenüber dieser allgemein üblichen Verfahrensweise ist in der DE-PS 3927 270 beschrieben.

Hierbei werden die Schlüsselgeheimnisse vorpersonalisiert und in Schlüsselmedien abgelegt. Diese so vorpersonalisierten Schlüsselträger werden an dezentralen Ausgabestellen bevorratet. In einem späteren Arbeitsgang werden die Zertifikate zentral erzeugt und über einen sicheren Kanal in die zugehörigen Medien abgespeichert.

Mit der Erfindung soll erreicht werden, daß die Schlüsselträger mit einem unpersonalisierten vertraulichen elektronischen Schlüssel und zugehörigen Zertifikaten in unbegrenzter Zahl im Vorlauf erzeugt und verteilt werden können, ohne die Zertifikate bei der Personalisierung mit dem Geheimnis zusammen in einen Schlüsselträger zu schreiben und ohne daß die Identität des späteren Inhabers oder die Anwendung bekannt bzw. festgelegt sind. Weiterhin soll es auch nicht notwendig sein, entsprechend dem verbesserten Verfahren die Zertifikate später nachzuladen.

Diese Aufgabe wird erfindungsgemäß durch die im Kennzeichen des Patentanspruchs 1 beschriebene Verfahrensweise gelöst.

Vorteilhafte Weiterbildungen des Verfahrens sind in den Kennzeichen der Unteransprüche 2 und 3 beschrieben.

Im Gegensatz zu bisherigen Ansätzen werden in diesem Verfahren die Anwendungszuordnungen nicht im Schlüsselträger vermerkt. Allein der Betreiber einer Anwendung bestimmt und verwaltet die Teilnahmeberechtigungen mittels der durch das Kryptoverfahren bereitgestellten festen Verknüpfung von Geheimnis und Zertifikat.

Die Realisierungsmöglichkeiten und Vorteile der Erfindung werden im nachfolgenden Ausführungsbeispiel näher erklärt.

Eine Schlüssel ausgebende Instanz erzeugt beliebig viele Schlüsselträger mit Schlüssel zur Deckung des voraussichtlichen Bedarfs. Die geheimzuhaltende Komponente wird dabei in den besonders geschützten Bereich eines Trägermediums gespeichert. Dazu wird ein Erzeugersiegel und eine Referenzinformation in den weniger gesicherten Bereich abgelegt. Die Referenz wird als Identifikation auf dem Schlüsselmedium visualisiert (z.B. auf den Schlüsselträger aufgedruckt). Das Geheimnis wird danach entweder vernichtet, oder getrennt mehrfach gesichert archiviert.

Die so erzeugten Schlüsselträger werden mit einer allgemeingültigen Hersteller-PIN versehen und bevorratet. Die fest zugehörige öffentliche Schlüsselkomponente wird zusammen mit einer zweiten Referenzinformation bei der ausgebenden Instanz gespeichert. Dabei gilt, daß die erste Referenz auf dem geheimen Teil ungleich der zweiten Referenz auf dem öffentlichen Teil ist.

Die Personalisierungsinstanz verwaltet die Verknüpfung der beiden Referenzen. Die Verknüpfung ist nur dem Personalisierer und dem rechtmäßigen Inhaber des Schlüssels bekannt.

Soll ein Schlüssel einem Benutzer zugeordnet, d. h. personalisiert werden, muß dessen Identität dem Personalisierer eindeutig bekanntgemacht und belegt werden. Anschließend bekommt der Interessent einen beliebigen Schlüsselträger mit der Aufforderung ausgehändigt, sofort nach Erhalt die Hersteller-PIN auf eine Individual-PIN zu ändern und den Empfang schriftlich zu bestätigen. Mit diesem Vorgang wird der Schlüsselträger physikalisch einer Person zugeordnet. Die außen erkennbare Referenz wird dem Auftraggeber zugeordnet.

Nach Eingang der Empfangsbestätigung reproduziert die Personalisierungsinstanz mittels der Referenzverknüpfung die öffentliche Schlüsselkomponente, zertifiziert die Verknüpfung des öffentlichen Teils mit der Benutzeridentität, stellt das Zertifikat in das öffentliche Schlüsselverzeichnis ein und sendet dem Benutzer eine beglaubigte Kopie des Eintrages zu.

Will ein beliebiger Benutzer des Schlüsselsystems mit einem anderen vertraulich Informationen austauschen, benötigt er dessen Zertifikat bzw. die daraus resultierende öffentliche Schlüsselkomponente. Dazu stehen, je nach Realisierung, beliebige Suchkriterien (Name, Vorname, Zertifikatsnummer, usw.) zur Verfügung.

Wendet im anderen Fall ein Systembeteiligter seine geheime Komponente an (z.B. elektronische Signatur), kann er dem Empfänger der so bearbeiteten Information entweder das komplette Zertifikat oder auch ledig-

lich die Referenz darauf mitteilen. Als Zusatzinformation gibt der Erzeuger der Information die Herkunft des Schlüssels (Erzeugersiegel) an. Der Empfänger kann mit der öffentlichen Komponente aus dem mit übertragenen Zertifikat eine Verifikation durchführen, oder er besorgt sich dazu mittels der Referenz das Zertifikat aus dem öffentlichen Schlüsselverzeichnis.

Soll ein Schlüssel, bzw. ein Zertifikat, innerhalb einer neuen Umgebung (z.B. Zutrittskontrollanlagen, Kreditkartenanwendungen usw.) Gültigkeit bekommen, muß der Betreiber dieser Anwendung lediglich das Zertifikat anerkennen. Damit kann der Inhaber des zugeordneten Schlüssels an dieser Anwendung teilnehmen, ohne daß irgend ein Eintrag im Schlüsselträger notwendig ist. Eine andere Möglichkeit besteht darin, zu einem von einer vertrauenswürdigen Instanz ausgegebenen Schlüssel anwendungsbezogene Sub-Zertifikate zu erzeugen, zu verwalten und zu pflegen und damit geschlossene Anwendungen zu erzeugen.

Die auf Vorrat produzierbaren Schlüssel sind nicht besonders schutzbedürftig, da das Medium sein Geheimnis nicht preisgibt und es auch nicht mit einer bestimmten Identität verknüpft ist.

Dem Schlüssel braucht keine Individual-PIN zugeordnet zu werden. Somit entfällt auch die Erzeugung, Verwaltung und der getrennte Versand der PIN-Briefe.

Ausgegebene Schlüsselträger sind nicht offensichtlich einer bestimmten Identität zugeordnet. Deshalb kann ein solches Medium "offen herumliegen", denn die Zertifizierungsinstanz (hier das öffentliche Schlüsselverzeichnis) gibt auf Anfrage mit der Referenz auf den Träger (das Geheimnis) kein Zertifikat heraus. Selbst wenn der "Finder" eines solchen Schlüssels die PIN kennt, kann er das Referenzzertifikat nur erraten.

Schlüsselträger, die für Aufgaben innerhalb bestimmter Organisationen (z.B. Sachbearbeiter innerhalb einer Firma), ausgegeben werden, können ihre Zuordnung wechseln, ohne daß das Medium getauscht wird. Es wird lediglich ein neues Zertifikat erzeugt und zugeordnet. Das Schlüsselmedium wird übergeben und der neue Inhaber verändert die PIN.

Nach diesem Verfahren erzeugte Schlüssel sind in ihrer Funktionalität herkömmlichen Schlüsseln (von Schloß mit Schlüssel) sehr ähnlich und können wie solche behandelt werden. Ein offen irgendwo auf der Straße liegender Schlüssel stellt für den Finder keinen Wert dar, denn die Zuordnung zum Schloß ist ihm nicht bekannt.

Ein weiterer entscheidender Vorteil des Verfahrens liegt darin, daß der oft sehr begrenzte Raum zum Speichern von Schlüsseln im geeigneten Speichermedium (z.B. Chipkarten) besser ausgenutzt werden kann; denn die Anwendungszuordnung wird in den Anwendungsumgebungen festgehalten und belastet so nicht das Schlüsselmedium.

Die Schlüssel sind anwendungsneutral. Das bedeutet, daß ein Schlüssel in beliebig vielen Anwendungen Gültigkeit haben kann, ohne daß hierfür zusätzliche Eintragungen notwendig sind.

Die Schlüssel sind anonym, denn nur die Personalisierungsinstanz und der rechtmäßige Eigentümer kennen die Zuordnung zur Identität.

Bei einem notwendigen Wechsel des Zertifizierungsschlüssels können zu den bis dahin ausgegebenen Schlüsseln neue Zertifikate erzeugt werden, ohne auf die Schlüsselmedien zugreifen zu müssen.

Zu einem Schlüssel können mehrere Zertifikate existieren. Damit können geschlossene Benutzergruppen gebildet werden, ohne immer neue Schlüssel zu erzeugen.

Patentansprüche

1. Verfahren zur Erzeugung und Verteilung unpersonalisierter vertraulicher elektronischer Schlüssel, **dadurch gekennzeichnet**, daß die Schlüsselträger zur Bevorratung mit einer sichtbaren Referenzidentifikation und einer allgemeingültigen Hersteller-PIN versehen und mit einem Schlüssel vorproduziert werden, welcher eine geheimzuhaltende Komponente im besonders geschützten Bereich sowie ein Erzeugersiegel und eine Referenzinformation im weniger geschützten Bereich enthält, daß die fest zugehörige öffentliche Schlüsselkomponente zusammen mit einer zweiten ungleichen Referenzinformation bei der Ausgabeinstanz gespeichert werden und daß erst bei der Zuordnung eines Schlüssels zu einem Benutzer dieser die Hersteller-PIN in eine Individual-PIN ändert, den Schlüsselerhalt quittiert und seine Identität der Personalisierungsinstanz nachweist, welche die beiden Referenzen verwaltet, die öffentliche Schlüsselkomponente personalisiert, versiegelt, in das Schlüsselverzeichnis einträgt und dem Benutzer bestätigt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die sichtbare Referenzidentifikation einem Auftraggeber zugeordnet wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß mit Hilfe der öffentlichen Komponente bzw. dem Erzeugersiegel eine Verifikation durchgeführt wird.